UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
Plaintiff,	:	
v.		20 Cr. 15 (PKC)
	:	
VIRGIL GRIFFITH,	:	
Defendant.		

DEFENDANT VIRGIL GRIFFITH'S MOTION TO:
(1) DISMISS THE INDICTMENT OR, IN THE ALTERNATIVE, TO SUPPRESS ALL OF MR. GRIFFITH'S DATA THAT WAS LOADED ONTO PALANTIR; AND
(2) COMPEL THE GOVERNMENT TO PROVIDE FURTHER INFORMATION CONCERNING THE SCOPE OF ITS CONSTITUTIONAL VIOLATIONS

BRIAN E. KLEIN
KERI CURTIS AXEL
WAYMAKER LLP
777 S. Figueroa Street, Suite 2850
Los Angeles, California 90017
(424) 652-7800

SEAN S. BUCKLEY
KOBRE & KIM LLP
800 Third Avenue
New York, New York 10022
(212) 488-1200

Attorneys for Virgil Griffith

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

PRELIMINARY STATEMENT

The government's recently revealed misconduct merits dismissal of the indictment against defendant Virgil Griffith, or at the very least, suppression of all evidence retrieved from his social media accounts. While the full scope of the government's misconduct is yet unknown, what is known more than justifies the requested relief.

On August 24, 2021, in a publicly filed letter, the government informed the Court and defense that Mr. Griffith's data, which the government received as a result of search warrants issued to two social media companies, Twitter and Facebook, had been loaded onto a document review platform known as Palantir, and vast amounts of his most personal life details had been made widely accessible to *anyone* with a Palantir login credential. This was done despite the fact that the search warrants did not permit the government's retention of non-responsive data after it had concluded its review for the fruits and instrumentalities of the alleged crimes with which it has accused Mr. Griffith. This situation persisted for more than a year and a half, permitting anyone with a Palantir credential to indiscriminately rummage through *all* of Mr. Griffith's data (far in excess of the scope of the data the search warrants actually authorized to be reviewed and/or seized),[1] which the government had no authority to let anyone at all access. The government's letter attempts to make this sound like a simple technical problem. But that this is definitely not the case.

Moreover, this is not an isolated incident. Courts in this District (and at least one other) have chastised the government numerous times for its practice of storing and

[1] In making this application, Mr. Griffith does not concede that the search warrants were valid or actually authorized the search and seizure of any of the materials in question. Mr. Griffith explicitly reserves all rights in that regard, particularly as it relates to the government's proposed exhibits and the evidence it intends to adduce at trial.

reviewing search warrant returns on its document review platforms, like Palantir, for extended periods of time and without the most basic of protection protocols as violations of the Fourth Amendment. Nonetheless, the government has failed to take corrective action to ensure that future violations would not occur, as is evidenced by this latest admission. Moreover, the defense has requested additional information to better understand the scope and impact of this breach, but the government has declined to provide important information. The breach identified in the government's letter is undoubtedly a violation of Mr. Griffith's Constitutional rights.

Accordingly, the defense respectfully requests that the Court exercise its supervisory power to dismiss the indictment given the outrageous government conduct. Dismissal is warranted given the systematic and pervasive issues repeatedly identified in this District with respect to the government's handling of search warrant returns in derogation of the Fourth Amendment. Even after repeated censure by various courts, the government continues to shirk the requirements of the Fourth Amendment by searching evidence without a warrant. Since less drastic measures have not yet impressed upon the government the importance of the particularity requirement in its storage and searching of electronic evidence, the remedy of dismissal is warranted. Perhaps facing the dismissal of entire cases will finally impress upon the government the seriousness of its Constitutional violations and will ensure that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV.

In the alternative, and at a minimum, the defense respectfully requests that the Court suppress all data uploaded to Palantir in connection with this case. The government's letter states that it "does not intend to use in this prosecution any of the data accessed" improperly,

but that would appear to only cover data the government has already deemed irrelevant. The government's "fix" is nothing more than an empty concession, renders no consequences for its bad behavior, and does not go far enough to remedy the potential harm committed. This is the FBI's third case in this district alone where it has been caught using a document review platform to engage in wholesale violations of the Fourth Amendment. Anything less than suppression of *all* the Palantir evidence—not just the evidence the government had no plans to utilize at trial—would render the Fourth Amendment a mere formality in this District and permit the government to get away with, yet again, a severe constitutional violation.

Moreover, the defense should be entitled to additional relief as the full scope of the government's violations remains unknown. In the lead up to this motion, the defense requested the government provide additional information related to the violation, but the government has refused to provide certain critical information. For this reason, the defense respectfully requests, in addition to the relief requested above, that the Court order the government to do the following:

(1) Provide a detailed update on the continuing investigation into the breach referenced in the government's August 24, 2021 letter.

(2) Produce all communications involving this situation by and between the prosecution team, Palantir, and/or anyone who viewed Mr. Griffith's data hosted on Palantir. This request includes, among other things, all emails and text messages. The time period of this request is from the start of this case to the present.

(3) Produce all communications by and between the prosecution team and any other document platforms and/or hosting services that might be hosting data for the government in this case. This request includes, among other things, all emails and text messages. The time period for this request is from August 11, 2021 (the date the FBI case agent claims to have learned of the improper access) to the present.

BACKGROUND

On January 10, 2020,[2] the government secured search warrants for Mr. Griffith's purported Twitter and Facebook accounts, among other data. (8/24/21 Ltr. from USAO to J. Castel (the "Aug. 24 Letter") at 1 (Dkt. No. 132).) Mr. Griffith's purported Apple iCloud and Google accounts were also covered by search warrants secured that same day, and the warrants collectively covered broad swaths of Mr. Griffith's personal and sensitive information, including instant messages, emails, photographs, and videos.[3] (USAO_000305-07 [Apple]; USAO_00312-14 [Twitter]; USAO_00318-20 [Facebook]; USAO_00324-29 [Google].)

The search warrants were limited in scope to review by the government to locate any evidence, fruits, and instrumentalities of conspiracy to obstruct the lawful governmental functions of the United States Office of Foreign Assets Control ("OFAC") in violation of 18 U.S.C. § 371 and/or conspiracy to violate, and aiding and abetting and willfully causing others to violate the International Emergency Economic Powers Act ("IEEPA") in violation

[2] The government's letter identified the date on which Magistrate Judge Debra Freeman authorized the searches as January 10, 2019. (Letter at 1.) A review of the discovery reveals, however, that the search warrants were signed on January 10, 2020. (USAO_000304 [Apple]; USAO_000311 [Twitter]; USAO_000317 [Facebook]; USAO_000323 [Google].)

[3] The search warrants requested, among other things: (1) iCloud account: account information, connected devices, emails, instant messages, files, IP logs, and geolocation information; (2) Twitter account: account information, IP logs, Tweets, direct messages, photographs, interactions with other accounts (including "favorited" tweets, retweets, followers, and blocked accounts), geolocation data, and searches; (3) Facebook account: account information, photos, videos, profile information, friend lists, status updates, groups and networks, events, rejected "Friend" requests, messages, IP logs, "Likes," and searches; and (4) Google: account information, geolocation data, emails, documents, Google Drive content, messages, related Android devices, web history, Google alerts, and payments. (*See* USAO_000303-330.)

of 50 U.S.C. §§ 1701-1706, with respect to Mr. Griffith's travel to the DPRK and for no other purpose. (*Id.*) The probable cause statement in the affidavit filed in support of the search warrants was based entirely on Mr. Griffith's alleged "travel to the DPRK to attend and present at the 'Pyongyang Blockchain and Cryptocurrency Conference'" and Mr. Griffith's subsequent consensual interviews with the FBI about his alleged travel to the DPRK to attend the conference. (USAO_000288-290.)

The government received data from Apple, Twitter, Facebook, and Google on or about March 9, 2020 (the "Search Data"). (*Id.*) On March 13, 2020, the defense received the raw search warrant returns from Facebook, Google, and Twitter as three electronic files, each identified by a single "Bates"[4] number: USAO_001556, USAO_001557, and USAO_001558. (Letter at 1; *see also* 3/13/20 Ltr. from USAO to Defense Counsel.) On May 13, 2020, the defense received the search warrant returns from Apple as a single electronic file bearing Bates number USAO_001559. (5/13/20 Ltr. from USAO to Defense Counsel.) Based on its view of these productions, the defense understands that these companies did not respond in a targeted manner, but rather produced the entirety of Mr. Griffith's files without any ascertainable narrowing.

The defense was never notified before the August 24 Letter that the government had loaded any data onto a document review platform, like Palantir,[5] nor that the data was loaded

[4] As the Court likely knows, "Bates numbering, named for the Bates Automatic Numbering-Machine," generally "assigns an arbitrary unique identifier to each page." *See* https://en.wikipedia.org/wiki/Bates_numbering. In this case, however, the government has simply assigned Bates-types numbers in its discovery index to whole forensic images of databases or devices, each of which may contain terabytes of data on it.

[5] The government's description of Palantir as simply a "document review platform" is misleading in the same way that referring to Google as a "search engine" would be. (*See*

onto the platform with settings that provided access to the returns to persons outside of the prosecution team for purposes not limited to those the government described in the search warrant applications.

Between March 10, 2020 and September 14, 2020, personnel from the prosecution team reviewed the Search Data for responsiveness. (Aug. 24 Letter at 1.) On September 24, 2020, the government notified the defense that it would not "search the data [seized] again without further Court authorization" and that the data had been "set aside" and "segregated," although the letter did not specify where the segregated data would be housed. (*Id.*; s*ee also* 9/24/20 Ltr. from USAO to Defense Counsel at 1-2.). As is evident from the government's August 24 letter, there was no such segregation. Rather than return or remove the non-responsive materials that were not subject to the search warrants, the government maintained both responsive and *nonresponsive* data on Palantir servers from March 10, 2020 to August 17, 2021 (the date the government claims the materials were deleted by Palantir at its request), ***a period of a year-and-a-half***. (Aug. 24 Letter at 2.) Per the government, the issue of the data's unfettered accessibility only came to light when an FBI analyst conducting a separate investigation was able to access materials from Facebook and Twitter seized pursuant to the search warrants, but *not* marked responsive by the FBI. (*Id.*)

Aug. 24 Letter at 1.) Palantir Technologies, Inc. provides multiple services to the government, including software and data analytics that utilize artificial intelligence and machine learning. Indeed, it is unknown exactly how many federal databases Palantir aggregates, mines, and analyzes pursuant to its contracts with the government. The advantage of Palantir over a traditional legal document review platform (such as Relativity) is that the Palantir software can mine and analyze social media data in a way that traditional document reviewers cannot. *See, e.g.*, *United States v. Bundy*, No. 3:16-cr-00051-BR, 2016 WL 8856696, at *4 (D. Ore. Sept. 14, 2016) (describing the Palantir Mint software program and its analysis of Facebook data).

Upon further investigation, the government revealed that FBI agents and intelligence analysts working *separate* matters wholly unrelated to this case accessed the Twitter and Facebook data loaded by the FBI onto Palantir on at least four separation occasions: May 4, 2020; April 6, 2021; May 27, 2021; and August 11, 2021. (*Id.* at 2-3.) This was possible because rather than restricting access to it from the moment they were loaded onto the Palantir platform, the prosecution team chose to leave in place a default setting that gave unlimited access to anyone with a Palantir credential. (*Id.* at 2.) At least one of these access periods—May 4, 2020—was before the prosecution team had completed its review of the materials for responsiveness. (*Id.*) The other three access periods were more than a year after the Twitter and Facebook data had been provided and more than seven months after the materials were supposedly "set aside" and "segregated" to not be viewed "again without further Court authorization." (*Id.*) [redacted]

[redacted] The government does not specify in the August 24 Letter which system accessed the search warrant materials nor does it adequately explain why a database established for the reporting, sharing, tracking, and mitigating of counterterrorism-based incidents would have access to the search warrant materials returned in a criminal matter.

Finally, the government notes in its letter that "the manner in which data is stored and accessed" in Palantir is "complex" and so the preliminary investigation into how many different Palantir users accessed it may be "incomplete." (*Id.*)

APPLICABLE LAW

The Fourth Amendment to the United States Constitution provides that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated" and "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV; *see United States v. Voustianiouk*, 685 F.3d 206, 210 (2d Cir. 2012) (suppressing evidence when police officers searched apartments outside those specified in a warrant). These requirements are not mere "formalities," *Voustianiouk*, 685 F.3d at 210 (*quoting McDonald v. United States*, 335 U.S. 451, 455 (1948)), and they ensure that law enforcement agents are not given the latitude to engage in "general, exploratory rummaging" through a person's belongings and data. *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (*quoting Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *see United States v. Wey*, 256 F. Supp. 3d 355, 379-80 (S.D.N.Y. 2017) (holding "lengthy (and continuing) retention and indiscriminate review of the vast

trove of electronic materials" obtained under warrants required suppression).

The "general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant" as well. *United States v. Nejad*, 436 F. Supp. 3d 707, 733 (*quoting United States v. Ramirez*, 523 U.S. 65, 71 (1998)). A search "must be confined to the terms and limitations of the warrant authorizing it." *United States v. Pinto-Thomaz*, 352 F. Supp. 3d 287, 308 (S.D.N.Y. 2018) (*quoting United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988)); *see Nejad*, 436 F. Supp. 3d at 733. Where law enforcement agents exceed a warrant's authority in their searches of the evidence seized, the "normal remedy is suppression and return of those items." *Nejad*, 436 F. Supp. 3d at 733; *see Pinto-Thomaz*, 352 F. Supp. 3d at 308. But where there is "flagrant disregard of the warrant's terms[,]" the "drastic remedy of the suppression of all evidence seized" may be justified. *Pinto-Thomaz*, 352 F. Supp. 3d at 308-09; *see Nejad*, 436 F. Supp. 3d at 733. Flagrant disregard of the warrant occurs where law enforcement agents "effect a widespread seizure of items that were not within the scope of the warrant" and "do not act in good faith." *Pinto-Thomaz*, 352 F. Supp. 3d at 309 (*quoting United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d. Cir. 2000)); *see Nejad*, 436 F. Supp. 3d at 733; *United States v. Dupree*, 781 F. Supp. 2d 115, 156 (E.D.N.Y. 2011). Exclusion is particularly warranted where it would "deter" law enforcement from Fourth Amendment violations in the future as where there is evidence of "deliberate, reckless, or grossly negligent conduct" or "recurring or systemic negligence."

Wey, 256 F. Supp. 3d at 394-95 (quoting *Herring v. United States*, 555 U.S. 135, 144 (2009)).

Where, as here, the evidence seized was electronic in nature, "the particularity requirement assumes even greater importance." *Galpin*, 720 F.3d at 446; *see Wey*, 256 F.

Supp. 3d at 383. The "potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous." *Galpin*, 720 F.3d at 447. Because there is essentially "no way to ascertain the content of a file without opening it" and "because files containing evidence of a crime may be intermingled with millions of innocuous files," the government's review of electronic evidence often requires the government to sift through gigabytes, if not terabytes, of data that is innocuous and completely irrelevant to the particulars of the search warrant at issue. *Id.* (*quoting United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010)). Without proper protocols, there is thus a "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *Id.* As such, the Court should have a "heightened sensitivity to the particularity requirement in the context of digital searches." *Id.* This is precisely why courts have held that, although the government is given latitude pursuant to Federal Rule of Criminal Procedure 41(e)(2)(B) to seize and copy electronically stored information for later review, such review must be completed within a "reasonable" period of time. *Wey*, 256 F. Supp. 3d at 383; *see Nejad*, 436 F. Supp. 3d at 735 ("As both parties recognize, the review must also have been completed in a reasonable amount of time to comply with the Fourth Amendment and Rule 41's requirements governing the execution of search warrants.")

A court can dismiss an indictment for outrageous government conduct that violates a defendant's Fifth Amendment right to due process. *See, e.g., United States v. Russell*, 411 U.S. 423, 431-32 (1973) ("[W]e may some day be presented with a situation in which the conduct of law enforcement agents is so outrageous that due process principles would absolutely bar the government from invoking judicial process to obtain a conviction."). To

warrant dismissal of an indictment, the outrageousness of such conduct must rise to the level of "government action that is fundamentally unfair or shocking to our traditional sense of justice" or conduct that is "so outrageous that common notions of fairness and decency would be offended were judicial processes invoked to obtain a conviction against the accused." *United States v. Schmidt*, 105 F.3d 82, 91 (2d Cir. 1997) (*quoting Kinsella v. United States ex rel. Singleton*, 361 U.S. 234, 246 (1960) and *Russell*, 411 U.S. at 431-32).

Although a court *can* dismiss an indictment for outrageous violations of a defendant's Fourth Amendment, at a minimum, it *should* suppress the evidence obtained (or in this case, impermissibly retained) by the government in violation of the Fourth Amendment. To safeguard the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," U.S. Const. amend. IV, the government cannot use "evidence obtained in violation of the Fourth Amendment" against the "victim of the illegal search and seizure." *United States v. Calandra*, 414 U.S. 338, 347 (1974). The prophylactic remedy of suppression is not intended to protect individuals like Mr. Griffith, whose privacy rights have already been undeniably violated by the government,[6] but "to deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment against unreasonable searches and seizures." *Calandra*, 414 U.S. at 347; *see United States v. Mazzara*, 2017 WL 4862793, at *7 (S.D.N.Y. Oct. 27, 2017) ("The purpose of excluding evidence seized in violation of the Fourth Amendment is to ensure judicial integrity and protect courts from being made a party to lawless invasions of the constitutional

[6] "The ruptured privacy of the victims' homes and effects cannot be restored. Reparation comes too late." *Calandra*, 414 U.S. at 347 (quoting *Linkletter v. Walker*, 381 U.S. 618, 637 (1965) (internal quotation marks and parentheses omitted).

rights of citizens by permitting unhindered governmental use of the fruits of such invasion.") (internal quotation marks and citation omitted).

Although the remedy of exclusion is "harsh," it is warranted where the government's misconduct is deliberate such that exclusion can "meaningfully" deter the misconduct in the future. *Mazzara*, 2017 WL 4862793, at *7 (quoting *Herring v. United States*, 555 U.S. 135, 144 (2009)); *see Calandra*, 414 U.S. at 348 ("The rule['s] purpose is to deter – to compel respect for the constitutional guaranty in the only effectively available way – by removing the incentive to disregard it.") (*quoting Elkins v. United States*, 364 U.S. 206, 217 (1960)). The government's conduct is sufficiently "deliberate" where it is "deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Herring*, 555 U.S. at 144, 147; *see Wey*, 256 F. Supp. 3d at 395. If a "law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment," suppression is warranted. *Id.* at 143 (*quoting Illinois v. Krull*, 480 U.S. 340, 348-49 (1987)).

ARGUMENT

I. The Court Should Dismiss the Indictment for Outrageous Government Conduct Given the Government's Systemic and Pervasive Issues Handling of Data It Is Not Entitled to Have.

There can be no other conclusion than that the government's poor maintenance of the Twitter and Facebook data—including materials considered *not* responsive—on a database which made the entirety of the returns accessible to anyone with access credentials to Palantir, and the FBI's searching of those materials for information unrelated to this case, was a violation of Constitutional rights. *See United States v. Nejad*, ___ F. Supp. 3d ___, 2021 WL 681427, at *8 (S.D.N.Y. Feb. 22, 2021) (finding that searches that did not conform

to the warrants on an FBI document review database were unconstitutional); *United States v. Nejad*, 487 F. Supp. 3d 206, 210 (S.D.N.Y. 2020) ("[R]eview of search warrant returns must be done in conformity with the warrants themselves."); *United States v. Nejad*, 436 F. Supp. 3d 707, 736 (S.D.N.Y. 2020) ("[S]earches conducted subsequent to the completion of the responsiveness review violated the Fourth Amendment"); *see also Wey*, 256 F. Supp. 3d at 379-80 (S.D.N.Y. 2017) (holding "lengthy (and continuing) retention and indiscriminate review of the vast trove of electronic materials" obtained under warrants required suppression); *United States v. Metter*, 860 F. Supp. 2d 205, 215 (E.D.N.Y. 2012) (finding that government's "blatant disregard" for its responsibility to determine which of the electronic data it seized was irrelevant was "unacceptable and unreasonable"). Given that this is the government's *third* case in *this* district in which it has categorically, and without good explanation, violated a criminal defendant's Fourth Amendment rights by searching and seizing electronic data outside the scope of a search warrant, the government's conduct has risen to the level of both shocking and outrageous. *See Schmidt*, 105 F.3d at 91. To permit the government to proceed to trial against Mr. Griffith when it has continually treated the Fourth Amendment as a passing fancy—as opposed to a severe constitutional restriction—would severely undermine our "common notions of fairness and decency" and thus the indictment should be dismissed pursuant to the due process clause of the Fifth Amendment. *See id.*

The search warrants authorized searches *only* for material pertinent to Mr. Griffith's alleged violations of the IEEPA and obstruction of OFAC's functions and any search outside of those parameters was wholly unauthorized and a violation of his rights under the Fourth Amendment. *See Nejad*, 487 F. Supp. at 210; *Wey*, 256 F. Supp. 3d at 408 (stating that the

government is not permitted to "sit" on terabytes of data for "years" and "intentionally mine it with searches targeting individuals and charging theories absent from the warrant application").

Further, the government's "retention of items outside the scope of the warrant[s]" was unconstitutional because documents "not identified as responsive at the conclusion of [responsiveness] review [fell outside] the scope of the warrant[s] and thus were not seized pursuant to them." *Nejad*, 436 F. Supp. 3d at 736 (citation and internal quotation marks omitted); *see Wey*, 256 F. Supp. 3d at 406 (stating that a subsequent search of documents judged irrelevant to the warrant "would have been presumptively impermissible"). As described above, the government completed its review of the Twitter and Facebook data almost a year ago. But rather than return the irrelevant electronic materials that did not fall within the scope of the warrants (and therefore it was not entitled even to possess), the government maintained the unresponsive materials on its data review platforms so that anyone with the right Palantir credentials could conduct warrantless searches of it. The government's proposed "fix" of not using only the improperly accessed data is nothing more than an empty gesture. The government never had any intention of using that data at trial in this case. Thus, the government is proposing a fix that would require it to suffer no consequences for the constitutional violations it has committed in this case, let along the aggregated constitutional violations it has committed with respect to defendants' Fourth Amendment rights in this district.

Moreover, the government's attempt to cast this issue as a simple, inadvertent mistake (an apparent attempt to invoke the good faith exception to the warrant requirement) rings hollow, particularly in light of similar past offenses committed by the government in other

cases in this district. Just this year, the government represented to another court in this District that it "implement[ed] new training protocols for prosecutors and FBI case agents" to "improve its infrastructure for data management and disclosure." *Nejad*, 2021 WL 681427, at *2. This was required because, in *Nejad*, the FBI did something incredibly similar what it did here: it uploaded "raw email search-warrant returns into its 'BIDMAS' database and searched [that] database hundreds of times" in violation of the Constitution's warrant requirement. *Id.* The district court therefore found that not only was this behavior in violation of the defendant's Fourth Amendment rights, but it "raise[d] questions about the FBI's attention to the limits of the Fourth Amendment in its use of the BIDMAS system more broadly." *Id.* at *9.

Evidently, the FBI did not learn—despite ample and detailed warnings from the other courts in this District—from its prior and intentional violations of a defendant's Fourth Amendment rights in cases such as *Nejad*. Consequently, during the time that Mr. Griffith's personal data has been on Palantir, it repeatedly has been accessed by FBI agents and analysts outside of the prosecution team, including data that was outside the scope of the search warrants and therefore the government had no right to have. These are patent violations of Mr. Griffith's Constitutional rights. Just as the good faith exception would not have saved the prosecution team in *Nejad* (who were saved, rather, by the U.S. Attorney's Office's agreement to dismiss the indictment), it should not save the prosecution here. *See Wey*, 256 F. Supp. 3d at 408 ("[G]ood faith is not a magic lamp for police officers to rub whenever they find themselves in trouble.") (*quoting United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996)). No amount of corrective prose by the courts in this district have caused the FBI to cease its severe dereliction of defendants' Fourth Amendment rights, nor has the

USAO's decision to willingly dismiss the indictment in *Nejad*. Only a dismissal, with prejudice, of a high-profile case may cause the government to cease its shocking and unfair decisions to maintain search warrant returns that were outside the scope of the search warrants on a database accessible to multiple other persons within the government, to access on any case at any time. This is the situation in which the repeated conduct of law enforcement agents was so "outrageous" that due process principles were violated. *Russell*, 411 U.S. at 431-32.

If this were the first case in which the FBI's use of document review platforms had resulted in wholesale abandonment of the Fourth Amendment's particularity requirements, dismissal of the indictment might not be warranted. However, this is at least the FBI's *third* case of misuse of its document review platforms in this district alone.[7] *See, e.g.*, *United States v. Nejad*, 487 F. Supp. 3d 206 (S.D.N.Y. 2020); *Wey*, 256 F. Supp. 3d 355. It appears that despite repeatedly being reprimanded for its failures, the FBI has done nothing, not even the simplest of fixes, to prevent these Fourth Amendment violations from recurring. They certainly did not do so in Mr. Griffith's case here. At a minimum, as more fully detailed below, this repeated misuse of the government's document review systems to violate is, at best, the type of systemic negligence that warrants wholesale suppression of all evidence loaded onto the document review platforms. *See Herring*, 555 U.S. at 144, 147; *Wey*, 256 F. Supp. 3d at 395.

[7] This includes the FBI's egregious misuse of the BIDMAS document review platform in *Nejad*, an unidentified document review platform in *Wey*, and now, the Palantir system. The government was also chastised for misusing the Palantir system in the District of Oregon in *Bundy*, 2016 WL 8856696.

The government wields "enormous prosecutorial power" and they "must exercise it in a way that is fully consistent with their constitutional and ethical obligations." *United States v. Nejad*, 487 F. Supp. 3d 206, 208 (S.D.N.Y. 2020). Where they fail to do so, as the government has done here, "it is the obligation of the courts" to "hold them accountable if they do not." In *Nejad*, the U.S. Attorney's Office appropriately chose to dismiss the indictment when it became clear that there were multiple constitutional violations that were legally unsupportable. The violations at issue here are parallel to the concerns that arose in *Nejad*. If the U.S. Attorney's Office will not dismiss this indictment voluntarily, then the Court should exercise its supervisory power and do so based on the blatant disregard for Mr. Griffith's Fourth Amendment rights.

II. The Court Should Suppress All the Data Loaded onto Palantir.

Alternatively, this Court should suppress all of Mr. Griffith's data that was loaded onto the Palantir database. The manner in which the government retained Mr. Griffith's Twitter and Facebook data, both the materials allegedly responsive to the search warrants and that which was not responsive, on the Palantir system for a period of more than a year and a half, which permitted anyone with an access credential to Palantir to view *all* of Mr. Griffith's data, was patently unconstitutional, lacking in good faith, and requires all of the evidence loaded onto Palantir to be suppressed. *See Nejad*, 436 F. Supp. 3d at 736-37. As noted above, this is the *third* case in *this* district alone in which the FBI has egregiously mishandled a defendant's private, sensitive data by retaining non-responsive materials on document review platforms in flagrant disregard for the scope of the search warrants. In both *Nejad* and *Wey*, other courts in this district have found that such deliberate, systemic disregard for the Fourth Amendment warrants suppression of all evidence seized. *Nejad*,

2021 WL 681427, at *9 ("[I]n light of the facts in this case, queries of information in the BIDMAS system may represent a blind sport in the Government's attention to its Fourth Amendment and *Brady* obligations.")[8]; *Wey*, 256 F. Supp. 3d at 409 ("[T]he Court concludes that suppression of all evidence seized during the course of both Searches is the only appropriate recourse under the circumstances."). If this is not the type of "systemic negligence" that justifies the exclusionary rule, then nothing is. *Herring*, 555 U.S. at 144, 147; *see Wey*, 256 F. Supp. 3d at 395.

Indeed, in *Bundy*, a District of Oregon case involving Facebook evidence loaded by the FBI onto Palantir, the district court held that a six-week delay between the government's completion of review under the warrant and the beginning of government's effort to locate and destroy or seal nonresponsive information "was unreasonable" under the Fourth Amendment. *Bundy*, 2016 WL 8856696, at *11. Although the government claimed to have conducted its responsiveness search in sixth months and that it had segregated non-responsive data (*i.e.*, data it was not entitled to have because it did not fall within the warrant), in fact it did not segregate the material for almost a year later. Accordingly, the FBI had plenary access to Mr. Griffith's person data to conduct warrantless searches for almost a year and a half. As in *Bundy*, this Court should be "troubled by the failures of the various agents, collectively and individually, to destroy or to seal information in their possession that was determined to be nonresponsive to the Warrant." *Id.*

[8] Notably, in *Nejad*, the U.S. Attorney's Office dismissed the case before that court could suppress all of the evidence in the BIDMAS system. However, given that court's most recent opinion, 2021 WL 681427, it is clear that would have been the result had the government been forthcoming with the court about its Constitutional violations.

Here, the period of time the government maintained data outside the scope of the search warrants was *far* longer and the government also permitted *anyone* with a Palantir access credential to access the *raw, native* search warrant returns (*i.e.*, both the responsive and non-responsive material). Given this court has already told the U.S. Attorney's Office and the FBI that such behavior is absolutely unconstitutional under the Fourth Amendment, this behavior is not merely "troubling," it is further evidence of a "blind sport in the [g]overnment's attention to its Fourth Amendment[.]". *Nejad*, 2021 WL 681427, at *9. Suppressing just the non-responsive Twitter and Facebook data, which the government essentially says it will do and which it has no plans to utilize at trial anyway, does nothing to deter the FBI from continuing its bad behavior. It must be deterred now, or else the protections of the Fourth Amendment in this District become little more than a mere formality. *See Voustianiouk*, 685 F.3d at 210.

Because the government permitted all of Mr. Griffith's data loaded onto Palantir to become subject to indiscriminate fishing by anyone with Palantir access credentials, should this Court not dismiss the indictment, the defense respectfully requests that all the data obtained through the search warrants and uploaded onto the Palantir database be suppressed and the government excluded from using this evidence at trial.

III. The Court Should Order the Government to Provide a Comprehensive Summary of the Scope of the Constitutional Violations.

As of the date of this motion, and by the government's own admission, it has not chronicled the full extent of its violations of Mr. Griffith's Fourth Amendment rights. The defense needs such information to properly assess the government's breaches and to consider additional motions or grounds for relief. Before filing this motion, the defense sought such

additional information directly from the government. Although the government provided some of the requested information (so the meet-and-confer process was partially successful), it did not provide the bulk of what is needed. The following are the outstanding defense requests, and the rationale for each request:

(1) Provide a detailed update on the government's continuing investigation referenced in your letter.

The government's August 24 letter states the government is "continuing to investigate" this matter. In response to the defense's request for an update, the government wrote: "the [g]overnment is continuing its inquiry into this matter and will update the Court accordingly, as indicated in our initial disclosure." This answer is non-responsive. Mr. Griffith has a right to know the results of the continuing investigations to understand the entire extent of the government's Constitutional violations.

(2) Produce all communications involving this situation by and between the prosecution team, Palantir, and/or anyone who viewed Mr. Griffith's data hosted on Palantir. This request includes, among other things, all emails and text messages. The time period of this request is from the start of this case to the present.

This information is critical for the defense to understand what exactly happened from the moment the data was upload, to the discovery of the violations, and through the present so that Mr. Griffith can adequately determine whatever legal claims and challenges are available to him. The information requested would also allow Mr. Griffith to assess what, if any, corrective action was taken, how quickly it was taken, and the sufficiency of any corrective action in attempting to ameliorate the Fourth Amendment violations.

(3) Produce all communications by and between the prosecution team and any other document platforms that might be hosting data for the government in this case. This request includes, among other things, all emails and text messages. The time period for this request is from August 11, 2021 (the date the FBI case agent claims to have learned of the improper access) to the present.

This information is vital for the same reason described in Request 2 immediately above.

The Court should compel the government to provide the requested information and documents so that the defense can properly and fully assess the total impact of the government's actions on Mr. Griffith's Constitutional rights.

CONCLUSION

For all the foregoing reasons, the defense respectfully requests that the Court grant dismiss the indictment (or in the alternative suppress all the evidence loaded onto Palantir) and compel the government to provide the requested additional discovery.

Dated: September 10, 2021

Respectfully Submitted,

/s/ Brian E. Klein

_____

Brian E. Klein
Keri Curtis Axel
Waymaker LLP

-and-

Sean S. Buckley
Kobre & Kim LLP

Attorneys for Virgil Griffith